Department of Homeland Security
Information Analysis and Infrastructure Protection
Daily Open Source Infrastructure Report for 20 June 2003

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The New York Times reports more than 100 members of the Municipal Credit Union were charged on Wednesday with looting hundreds of thousands of dollars from automated teller machines when a computer failure caused by the collapse of the World Trade Center allowed virtually unlimited access to money. (See item 4)
- CNN reports an Ohio truck driver accused of plotting a terror attack on New York City's Brooklyn Bridge has agreed to plead guilty to providing material support to a terrorist organization. (See item 5)
- The Register reports Sobig−D, a new variant in the Sobig worm series, appeared Wednesday, and infectious emails sent out by the worm appear to come from admin@support.com. (See item 18)

DHS/IAIP Update *Fast Jump*

Production Industries: Energy; Chemical; Defense Industrial Base
Service Industries: Banking and Finance; Transportation; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information and Telecommunications; Internet Alert Dashboard
Other: General; DHS/IAIP Web Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 19, Reuters* — **Small amount of plutonium missing from Los Alamos. The Los Alamos nuclear laboratory said on Wednesday a small amount of low−grade plutonium turned up missing after a transfer of the material that is used to make nuclear bombs, but added the missing plutonium does not pose a threat.** "The total amount of nuclear material involved is very small, but due to security requirements the specific quantity cannot be disclosed," Los Alamos National Laboratory said in a statement. A watchdog group called Project on Government Oversight said the missing material consisted of two grams (0.0755

ounce) of weapons−grade plutonium. A Los Alamos spokesman said the missing material was not weapons grade. **Los Alamos officials said they discovered the disappearance of the material −− two low−purity analytical samples of plutonium−oxide −− last Thursday and the lab is conducting a complete material inventory.** Lab officials believe the nuclear material was likely discarded as a residue through approved processes.
Source: http://asia.reuters.com/newsArticle.jhtml?type=scienceNewsstoryID=2952653

2. *June 18, Platts Global Energy News* — **Domenici: easier to build reactor now than 20 years ago. Construction of new power reactors will be much easier now than it was 20 years ago,** Sen. Pete Domenici (R−NM) said today. The chairman of the Energy & Natural Resources Committee, who met with reporters to discuss the Senate's comprehensive energy bill, pointed to the untested streamlined licensing process at NRC that was mandated under a 1992 federal law. **The streamlining is expected to help reduce the cost and time needed to build a new reactor.** Domenici stressed the U.S. cannot meet the projected growth in electricity demand "without something like nuclear power plants." He appeared hopeful that provisions authorizing federal loan guarantees for new reactors, which were attached to the Senate energy bill last week following a 50−48 vote, would not be a contentious item during a House−Senate conference committee.
Source: http://www.platts.com/stories/nuclear2.html

[Return to top]

Chemical Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *June 19, Computerworld* — **Streamlined communications called key to homeland security.** Streamlined and secure information management is a critical element for the U.S. Northern Command in providing homeland defense of North America when it assumes its full operational role October 1. **Army Lt. Gen. Edward Anderson III, the deputy commander of the Northern Command, based at Peterson Air Force Base in Colorado Springs, said efficient communications has been an objective since the command was established October 1, 2002.** "The intent is to move information out of traditional military stovepipes and to share the information with all that need it," Anderson said to an audience of military and civilian information security professionals at the Federal Information Superiority Conference in Colorado Springs this week. "We take information from a multitude of sources and process it for a multitude of uses," Anderson said. "Information−sharing is absolutely key" to the Northern Command's mission of providing military support for local, state and federal authorities. **Managing the command's information is the responsibility of the Information Synchronization Group, which reports to Air Force Gen. Ralph Eberhart, head of the Northern Command.**
Source: http://www.computerworld.com/printthis/2003/0,4814,82244,00. html

[Return to top]

Banking and Finance Sector

4. *June 19, New York Times* — **118 charged in ATM thefts after 9/11.** More than 100 members of the Municipal Credit Union were charged on Wednesday with looting hundreds of thousands of dollars from automated teller machines (ATM) when a computer failure caused by the collapse of the World Trade Center allowed virtually unlimited access to money, prosecutors said. Charges of grand larceny were filed against 118 credit union members, including city employees, health care workers and education workers, who are accused of stealing at least $5,000 each in the chaos of September 11, 2001, and its aftermath. The authorities said each could face up to seven years in prison if convicted. **A frenzy of withdrawals began almost immediately after the attack, when the credit union, which has its headquarters on Cortlandt Street near ground zero, lost its computer link to the New York Cash Exchange, a network that processes ATM transactions. The network had no way to check the credit union accounts to ensure that there was sufficient funds to cover the withdrawals, credit union officials have said.** Rather than shut down its ATM operation, and believing that it was helping its members during a crisis, it continued to allow withdrawals without knowing whether those making the withdrawals had sufficient money in their accounts, the credit union has said.
   Source: http://www.nytimes.com/2003/06/19/nyregion/19UNIO.html

[Return to top]

Transportation Sector

5. *June 19, CNN* — **Ohio trucker pleads guilty to al Qaeda ties. An Ohio truck driver accused of plotting a terror attack on New York City's Brooklyn Bridge has agreed to plead guilty to providing material support to a terrorist organization, Attorney General John Ashcroft announced on Thursday.** Ashcroft said Iyman Faris "appeared to be a hard−working truck driver," but traveled to Pakistan, met with Osama bin Laden in Afghanistan, and "joined al Qaeda's jihad against America." The charges together carry as much as 20 years in prison and up to $500,000 in fines. **Al Qaeda leader Khalid Shaikh Mohammed, who is in U.S. custody, has told interrogators that Faris was ordered to perform surveillance of the Brooklyn Bridge with the ultimate goal of cutting its cables,** sources told CNN. Ashcroft said **Faris scouted potential terror targets from April 2002 to March 2003, and said he had provided al Qaeda with research on ultralight airplanes in early 2001.** Ascroft also said Faris gave al Qaeda material support including "dealings involving cash, thousands of sleeping bags, plane tickets and cell phones." He was also allegedly involved in a plot to drive a truck loaded with explosives onto an airport tarmac to blow up a plane, sources said. Neither alleged plan was executed. The arrest of Faris and the plea deal, reached on May 1, was kept secret because of the sensitivity of the case, CNN has confirmed.
   Source: http://www.cnn.com/2003/LAW/06/19/alqaeda.plea/

6. *June 19, The Atlanta Journal−Constitution* — **Delta to test electronic tags to help track baggage.** Delta Air Lines hopes to track passengers' baggage using radio signal technology.

The airline this fall will test the use of small chips embedded in bag tags on certain flights from Jacksonville. **Using Radio Frequency Identification technology, radio signals broadcast from a reader would send and receive information from the chips. Delta said the system could help it better track baggage and cargo.** The 30−day test will involve more than 40,000 900MHz disposable tags provided by Matrics of Columbia, Md. and SCS Corporation of San Diego, Calif. It will be conducted in coordination with the Transportation Security Administration. **Delta said the radio−tracking project is part of an airport technology overhaul that also includes installation of more self−serve check−in kiosks and special phone help lines.**
Source: http://www.ajc.com/business/content/business/delta/0603/18ba gs.html

[Return to top]

Postal and Shipping Sector

7. *June 19, Federal Computer Week* — **DHS systems working to stop contraband. Brian Goebel, senior adviser at the Bureau of Customs and Border Protection, said the U.S. is succeeding in pushing its borders away from its shoreline and checking for potential terrorist contraband thousands of miles away.** And with increased surveillance of cargo containers at foreign ports, "we are in fact making seizures overseas," said Goebel, speaking at the Homeland Security Financing Briefing. Although Goebel declined to provide details, he did say that machine guns and gas masks were seized by law enforcement. He did not say where, but he did say, "The program is succeeding." **The agency, which is part of Department of Homeland Security (DHS), has implemented procedures designed to toughen inspections of cargo containers at foreign ports.**
Source: http://www.fcw.com/fcw/articles/2003/0616/web−dhs−06−19−03.a sp

[Return to top]

Agriculture Sector

8. *June 19, Washington Post* — **McDonald's asks meat suppliers to stop using antibiotics. McDonald's Thursday directed some meat suppliers to stop using antibiotic growth promoters altogether and encouraging others to cut back.** The new policy, the broadest in the U.S., focuses on the use of antibiotics in animal feed to speed the development of livestock, a practice widely seen by researchers as the least important and most expendable use of important antibiotics. **Because McDonald's is the nation's largest purchaser of beef and among the largest for chicken and pork, its action will noticeably reduce the amount of antibiotics being used as growth promoters.** The McDonald's policy will prohibit its direct suppliers from using 24 growth promoters that are closely related to antibiotics used in human medicine. The firm, in deciding which independent farmers will supply its beef, chicken, and pork, will consider it a "favorable factor" if the supplier avoids growth promoters.
Source: http://www.washingtonpost.com/wp−dyn/articles/A12881−2003Jun 19.html?nav=hptop_tb

[Return to top]

Food Sector

9. *June 16, Federal Times* — **Employees step up resistance to outsourcing efforts. A food inspection program run out of the Commerce Department that is viewed as important to homeland security may soon face privatization. The sign that the program may be privatized came when Commerce reclassified the 157 jobs in the program as commercial. In response, the seafood inspectors are waging an administrative battle to get themselves reclassified as inherently governmental, a designation that makes all those covered immune from possible outsourcing.** For the Seafood Inspection Program, the problem appears to be that it is unwanted by its parent agency. It is buried deep in the Commerce Department, it reports to the National Marine Fisheries Service, part of the National Oceanic and Atmospheric Administration (NOAA). And NOAA has repeatedly floated proposals to move the seafood program to another agency. Four years ago, the agency proposed transferring the program to the Food and Drug Administration, and it reiterated that suggestion in a report last year to the Office of Management and Budget.
   Source: http://federaltimes.com/index.php?S=1939931

[Return to top]

Water Sector

10. *June 18, Milwaukee Journal Sentinel* — **Wisconsin cutting back water rule enforcement. Wisconsin will scale back some enforcement of rules and testing requirements for roughly 12,000 public water systems that serve 4 million people because of staff and budget cuts, state water quality experts said Wednesday.** In addition, municipal water utility managers and private well owners will receive less assistance from the Department of Natural Resources Drinking Water and Groundwater Bureau, as the agency cuts more than 10 percent of its 115 workers. State funding for the bureau is expected to drop from $3.6 million in 2001 to $2 million in the upcoming fiscal year, cutting roughly $1.6 million from the agency's total annual budget of $10 million.
    Source: http://www.jsonline.com/news/state/jun03/149123.asp

[Return to top]

Public Health Sector

11. *June 18, New York Times* — **National programs to vaccinate for smallpox come to a halt. Government officials said today that both the civilian and military smallpox vaccination programs have virtually come to a halt, the military program because it has vaccinated everyone it can and the civilian program because few people volunteered for it. Officials also said that of the 493,000 people who had been vaccinated, the rate of dangerous side effects was lower than predicted.** The military has inoculated 454,856 personnel, nearly 90 percent of them before the invasion of Iraq and is now vaccinating about 1,000 a week. State health departments have inoculated 37,608 civilian emergency health workers and are adding about 100 more each week.

Source: http://www.nytimes.com/2003/06/19/politics/19POX.html

12. *June 18, Associated Press* — **D.C. anthrax cleanup cost $27 million. The Environmental Protection Agency (EPA) spent $27 million over three months to decontaminate Capitol Hill offices after the anthrax attack of October 2001, according to a congressional report released Tuesday. The report said the EPA originally estimated the cleanup cost at $5 million, but that figure was steadily revised upward as the complexity of the operation became clear.** Because of the uniqueness of the attack, "protocols for responding to contamination by anthrax or other biological agents did not exist." **There were uncertainties about the health risks involved, and the EPA and its contractors had to figure out how to decontaminate large areas within buildings with limited practical knowledge.** Senate Finance Committee Chairman Charles Grassley said the cleanup, "a huge challenge," was a success and no one was harmed, but he urged the EPA to follow up on recommendations to improve its contract tracking system to "ensure the government gets its money's worth out of contractors on these big projects."
Source: http://www.nytimes.com/aponline/national/AP−Anthrax−Cleanup. html

13. *June 18, Federal Computer Week* — **Wireless security entangles HIPAA.** The Health Insurance Portability and Accountability Act (HIPAA) is a federal law that is supposed to strengthen privacy procedures involving personal patient health and medical information, simplify administrative codes and standards for electronic data interchange, and improve security of networks handling such data. **Although most health organizations still have another 22 months to comply with new federal security standards, securing wireless networks may pose a problem as they near the deadline.** "There are so many security issues around wireless and the security rule gives you no substantial guidance on how to secure wireless," said Marne Gordon, director of regulatory affairs at TruSecure Corp., referring to the HIPAA guidelines on security.
Source: http://www.fcw.com/geb/articles/2003/0616/web−hipaa−06−18−03 .asp

14. *June 16, Ascribe Newswire* — **Work could result in treatment for smallpox, monkeypox. Molecular biologists from the University of Buffalo have discovered a novel way to inhibit the replication of poxviruses, the group that includes smallpox virus, by interfering with messenger RNA synthesis necessary for the viruses to reproduce in a host organism.** "Since poxviruses replicate in the cytoplasm, they can't use hosts enzymes present in the nucleus to make their proteins," said Edward Niles, professor of microbiology. "This quirk in the poxvirus replication process should make it possible for scientists to design drugs targeted to those unique viral enzymes without interrupting normal cellular functions," he said. **The discovery could lead to drugs that would be available to treat the potentially deadly disease if there were a bioterrorism−related outbreak. If a new smallpox vaccination campaign were undertaken, such drugs also could be available to treat persons who have serious reactions to the vaccine. Such drugs also would be effective against related poxviruses such as monkeypox.**
Source: http://www.ascribe.org/cgi−bin/spew4th.pl?ascribeid=20030613 .135413t>

[Return to top]

Government Sector

15. *June 19, U.S. Department of Homeland Security* — **Department of Homeland Security seal.** On Thursday Secretary Ridge unveiled the new Department of Homeland Security seal for the first time. **The seal was designed to be symbolic of the new Department's mission: to prevent terrorist attacks within the United States; reduce American's vulnerability to terrorism; and minimize the damage and recover from the attacks that do occur.** In the center of the seal, a graphically styled white American eagle appears in a circular blue field. The eagle's outstretched wings break through an inner red ring into an outer white ring that contains the words "U.S. DEPARTMENT OF" in the top half and "HOMELAND SECURITY" in the bottom half in a circular placement. **The eagle's wings break through the inner circle into the outer ring to suggest that the Department of Homeland Security will break through traditional bureaucracy and perform government functions differently.** In the tradition of the Great Seal of the United States, the eagle's left claw holds an olive branch with 13 leaves and 13 seeds while the right claw grasps 13 arrows.
Source: http://www.dhs.gov/dhspublic/display?content=1017

16. *June 19, Associated Press* — **Homeland security info sharing to take time.** It would be a daunting challenge for even the sharpest programming wizards: set up a secure computer network for the 190,000 workers in the Homeland Security Department. **It will take years to design and build a new system that unifies information−sharing at the reconstituted agencies now under one umbrella, said Edward Kinney, director of information technology for Customs & Border Protection. Compounding the challenge will be the task of keeping existing networks operational and secure during the transition.** Kinney spoke Wednesday at a conference that put government and private computer company representatives together to discuss security. He declined to provide specifics about the new network.
Source: http://www.washingtonpost.com/wp−dyn/articles/A11100−2003Jun 18.html

17. *June 18, General Accounting Office* — **Border Security: New policies and procedures are needed to fill gaps in the visa revocation process.** The General Accounting Office (GAO) on June 18 published Report GAO−03−798: New policies and procedures are needed to fill gaps in the visa revocation process. **According to the GAO's review, the U.S. government has no specific written policy on the use of visa revocations as an antiterrorism tool and no written procedures to guide State in notifying the relevant agencies of visa revocations on terrorism grounds.** In addition, State, INS, and the FBI do not have written internal procedures for notifying their appropriate personnel to take specific actions on visas revoked by the State Department. State and INS officials said they use the revocation process to prevent suspected terrorists from entering the county, but none of the agencies has a policy that covers investigating, locating, and taking action when a visa holder has already entered. **This lack of formal written policies and procedures has contributed to systemic weaknesses in the visa revocation process that increase the possibility of a suspected terrorist entering or remaining in the United States. The GAO recommends that when State revokes a visa because of terrorism concerns, the appropriate units within State, INS, and the FBI are notified immeidately and that proper actions are taken.** Highlights:
http://www.gao.gov/highlights/d03798high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−03−798

[Return to top]

Emergency Services Sector

Nothing to report.
[Return to top]

Information and Telecommunications Sector

18. *June 18, The Register* — **Fresh variant to Sobig worm.** A new variant in the Sobig series appeared Wednesday. Sobig−D is a little different from its predecessors the Sobig−B (support@microsoft.com) and Sobig−C (bill@microsoft.com) worms. **Infectious emails sent out by Sobig.D appear to come from admin@support.com. The worm is spreading modestly and causing only a minimal amount of damage**. Most vendors rate it as low risk. **Although it normally spreads via email, Sobig−D can also spread through network shares**. In its more common email form, Sobig−D appears as email with randomized subject lines (such as Re: Documents and Re: Movies) and carries infectious .scr and .pif attachments. Like its predecessors, **Sobig−D has a built−in expiration date−−in this case July 2**. Users should keep their anti−virus software updated.
Source: http://www.theregister.co.uk/content/56/31292.html

19. *June 17, Associated Press* — **Former Ericsson workers convicted of espionage. An engineer laid off in 2001 from wireless equipment maker LM Ericsson was sentenced Tuesday to eight years in prison for espionage**. Afshin Bavand handed secret company documents to Russian intelligence agents last year, an act that could have harmed Sweden's national security, the Stockholm district court said. Two of Bavand's co−workers at Ericsson were convicted of complicity in industrial espionage for gathering some of the information and giving it to Bavand. Prosecutors said Bavand received thousands of dollars as payment for passing thousands of secret documents to the agents. The court said **the documents contained "technical information with connection to mobile telephony and fixed telephony as well as to both existing and future systems."**
Source: http://www.usatoday.com/tech/world/2003−06−17−ericsson−verdi ct_x.htm

20. *June 16, Government Computer News* — **As threats rise, feds shelter their IT. The threat of cyberattacks on government systems is escalating** as computers become ever more interconnected, use of the Internet increases, and attack technology becomes ever more sophisticated and readily available. **Integrating security into enterprise architectures has emerged as a major theme, with the Office of Management and Budget (OMB) pushing agencies to build architectures and use them as tools to improve efficiency and organization**. "Agencies have to make sure [security] is in their enterprise architectures, in their business cases, and in their system administration, operations and support practices," said Mark Forman, the OMB's administrator for e−government and IT.
Source: http://gcn.com/22_15/news/22412−1.html

Current Alert Levels

 AlertCon: 1 out of 4 https://gtoc.iss.net	 Security Focus ThreatCon: 1 out of 4 http://analyzer.securityfocus.com/

Current Virus and Port Attacks

Virus:	#1 Virus in the United States: **WORM_LOVGATE.G** Source: http://wtc.trendmicro.com/wtc/wmap.html, Trend World Micro Virus Tracking Center [Infected Computers, North America, Past 24 hours, #1 in United States]
Top 10 Target Ports	137 (netbios−ns), 80 (www), 1434 (ms−sql−m), 445 (microsoft−ds), 113 (ident), 139 (netbios−ssn), 7338 (swx), 0 (−−−), 53 (domain), 25 (smtp) Source: http://isc.incidents.org/top10.html; Internet Storm Center

[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP web−site (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Warnings − DHS/IAIP Assessements, Advisories, and Alerts: DHS/IAIP produces three levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that address cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Publications − DHS/IAIP Daily Reports, CyberNotes, Information Bulletins, and other publications

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	nipcdailyadmin@mail.nipc.osis.gov or contact the DHS/IAIP Daily Report Team at 202−324−1129
Distribution Information	Send mail to nipcdailyadmin@mail.nipc.osis.gov for more information.

Contact DHS/IAIP

To report any incidents or to request information from DHS/IAIP, contact the DHS/IAIP Watch at nipc.watch@fbi.gov or call 202−323−3204.

DHS/IAIP Disclaimer